

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION**

Valencia R. Davis, individually and on behalf of all others similarly situated,  Plaintiff,  v.  Cinfed Federal Credit Union,  Defendant.	Case No.: 1:23-CV-776  <b>JUDGE</b>  <b>MAGISTRATE JUDGE</b>  <b>CLASS ACTION COMPLAINT AND JURY TRIAL DEMAND</b>
--	---

Plaintiff Valencia R. Davis, individually and on behalf of all others similarly situated, brings this action against Defendant Cinfed Federal Credit Union (“Cinfed” or “Defendant”), a community chartered federal credit union, to obtain damages, restitution, and injunctive relief for the proposed Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

**NATURE OF THE ACTION**

1. This class action arises out of the recent targeted cyberattack and data breach (the “Data Breach”) on Defendant’s network that resulted in unauthorized access to the sensitive data of its employees and customers. As a result of the Data Breach, Plaintiff and approximately 58,000 other individuals<sup>1</sup> (“Class Members”) suffered ascertainable losses in the form of invasion of privacy, the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

---

<sup>1</sup> <https://apps.web.maine.gov/online/aeviewer/ME/40/5148ba99-c8e9-42cc-bf51-400f9f032c68.shtml> (last visited November 10, 2023).

2. Information compromised in the Data Breach includes Defendant's clients' full names, Social Security Numbers, and financial account information (collectively referred to as "PII").<sup>2</sup>

3. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to unauthorized access, acquisition, and publication by an unknown third party, or specifying exactly what specific type of information was accessed.

4. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

5. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent, reckless, and intentional conduct since the PII that Defendant collected and maintained is now in the hands of data thieves who have already disseminated the information to additional third parties.

6. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' PII to target other phishing and hacking intrusions, using Class Members'

---

<sup>2</sup> *Id.*

information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

7. As a result of the Data Breach, Plaintiff and Class Members have suffered actual injury to their privacy.

8. Plaintiff and Class Members have also been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft and fraud.

9. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, trips to the bank, or other protective measures to deter and detect identity theft.

10. Plaintiff seeks remedies including, but not limited to, compensatory damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

11. Accordingly, Plaintiff bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of fiduciary duty, (iv) breach of confidence, (v) invasion of privacy, (vi) breach of implied contract, and (vii) unjust enrichment.

### **JURISDICTION AND VENUE**

12. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and

the amount in controversy exceed \$5,000,000, exclusive of interest and costs. At least 1 class members is a citizen of a different state than Defendant.

13. This Court has general personal jurisdiction over Defendant Cinfed Credit Union because Defendant's principle place of business is, and regularly conducts business, in Cincinnati, Ohio.

14. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1392(c)(2) as substantial part of the events giving rise to the causes of action brought in this action occurred within this District, and Defendant conducts substantial business in this District.

### **PARTIES**

15. Plaintiff Valencia R. Davis is and at all relevant times was a citizen of the Cincinnati, Ohio within Hamilton County. Plaintiff voluntarily conducted business with Defendant and still remains a customer as of the date of this Complaint.

16. Defendant Cinfed Federal Credit Union is a community chartered federal credit union with its principal place of business located at 4801 Kennedy Avenue, Cincinnati, Ohio 45209 within Hamilton County, that provides banking services to residents of seventeen (17) counties across Ohio, Kentucky, and Indiana. Defendant Cinfed has a registered agent, Jay Sigler, located at 550 Main Street, Suite 5500, Cincinnati, OH 45202.

### **BACKGROUND**

17. As a condition of employment and/or receiving banking services, Defendant requires Class Members to entrust it with highly sensitive personal information.

18. On information and belief, in the ordinary course of providing banking services, Cinfed requires clients to provide sensitive personal and PII such as: (1) name, address, phone number and email address; (2) date of birth; (3) demographic information; (4) state ID or drivers'

license; (5) Social Security Card; (6) Medicaid or other insurance card; (7) proof of income, such as a bank statement, pay stub, or W-2; (8) proof of residency, such as a utility bill; (9) proof of major medical expenses, child support, or alimony (if applicable); (10) custody or guardianship documents (for youth under 18 or adults with a legal guardian); (11) birth certificate (for youth under 18) and; (110 Other information that may be deemed necessary to provide services and treatment.

19. Similarly, on information and belief, Cinfed requires that its employees, partners, and other third parties provide sensitive personal and PII such as: (1) name, address, phone number and email address; (2) Date of birth; (3) demographic information; (4) Social Security number; (5) financial information; and (6) other information that may be deemed necessary for purposes of employment or affiliation.

20. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

21. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

22. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

23. Defendant Cinfed recognizes its obligation to protect the PII in its custody, stating that "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We select businesses that offer products to enhance your economic well-being.

We will never authorize these firms to charge your account without your consent. We do not sell to telemarketers.”<sup>3</sup>

24. Upon information and belief, Defendant provides (and is likely required by law to provide) a copy of its Privacy Policy to its customers

25. Because of the highly sensitive and personal nature of the information it acquires and stores with respect to its customers and employees, Defendant promises to (among other things): (1) make sure that financial and other information that identifies customers is kept private; (2) give customers notice of Defendant’s legal duties and privacy practices with respect to their Privacy Policy; (3) follow the terms of the Privacy Policy; (4) notify customers of any breaches of unsecured PII that may occur; and (5) adequately safeguard the PII of employees and customers that it requires them to provide.

#### **A. The Cyberattack and Data Breach**

26. On October 23, 2023, Cinfed confirmed it experienced a cybersecurity incident, which resulted in the Data Breach that exposed the PII of its customers and employees.<sup>4</sup>

27. According to Cinfed, its investigation “recently concluded and determined that an unknown, unauthorized third party gained access to Cinfed’s internal corporate network from September 22, 2023, to September 25, 2023, and, during that time, accessed certain documents in our network.”<sup>5</sup>

28. Defendant did not begin notifying victims of the Data Breach until November 9, 2023.

---

<sup>3</sup> <https://cdn.userway.org/remediations/pdf/291/e58707c4798a34ce.pdf> (last visited Nov. 17, 2023).

<sup>4</sup> <https://apps.web.maine.gov/online/aeviewer/ME/40/5148ba99-c8e9-42cc-bf51-400f9f032c68.shtml> (last visited November 17, 2023).

<sup>5</sup> *Id.*

29. The notices received by Plaintiff and the Class Members are vague and inadequate. For example, the notices fail to identify the specific information and records compromised, when the breach was discovered, how the breach occurred, how many people were affected, whether the information was encrypted, or the fact that their PII had already been publicly listed for sale on the internet and/or disseminated to third parties.

30. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. Defendant's data security obligations were particularly important given the sensitivity of the PII it maintained and substantial increase in cyberattacks and/or data breaches in the banking industry preceding the date of the breach.

32. The attacker accessed and acquired files on the server containing information including names, Social Security numbers, and financial account numbers.

33. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

34. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

35. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

36. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted

marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

38. Because Defendant had a duty to protect Plaintiff's and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

39. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

40. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

41. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers and employees, including Plaintiff and Class Members.

42. In April 2020, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," Ooda Analyst reported that "*[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies*." They breach networks, use specialized tools to maximize

damage, *leak corporate information on dark web portals*, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay.”<sup>6</sup>

43. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim (emphasis added), data and pressured victims to pay by threatening to release the stolen data.”

44. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals’ tactics included threatening to release stolen data.

45. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant’s type of business had cause to be particularly on guard against such an attack.

46. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff’s and Class Members’ PII could be accessed, exfiltrated, and published as the result of a cyberattack.

---

<sup>6</sup> OodaLoop, *Ransomware mentioned in 1,000+ SEC filings over the past year*, available at <https://www.oodaloop.com/briefs/2020/05/04/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/#:~:text=The%20agency%20states%20that%20in%20the%20past%20year%2C,days%20al one%20include%20American%20Airlines%2C%20McDonald%E2%80%99s%2C%20and%20Alphabet> (last visited Nov. 17, 2023).

47. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

**B. Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.**

48. Defendant acquired, collected, and stored the PII of Plaintiff and the Class.

49. As part of being a customer and/or an employee of Defendant, Plaintiff and Class Members, are required to give their sensitive and confidential PII to Defendant. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to conduct its business in the financial industry.

50. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

51. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

52. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."<sup>7</sup>

---

<sup>7</sup> See How to Protect Your Networks from RANSOMWARE, at 3, *available at* <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Nov. 17, 2023).

53. To prevent and detect cyberattacks, including the attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>8</sup>

54. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

---

<sup>8</sup> *Id.* at 3-4.

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want

to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....<sup>9</sup>

55. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

---

<sup>9</sup> See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited Nov. 17, 2023).

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].<sup>10</sup>

56. Given that Defendant was storing the PII of approximately 58,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

57. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of 58,000 individuals, including Plaintiff and Class Members.

**C. Securing PII and Preventing Breaches**

58. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to

---

<sup>10</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 17, 2023).

maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

59. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

60. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

61. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."<sup>11</sup> The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."<sup>12</sup>

62. Defendant knew and understood unprotected or exposed PII in the custody of financial companies and banks in the industry, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access, as these companies maintain highly sensitive PII of employees and consumers, including Social Security numbers and financial information.

---

<sup>11</sup> 17 C.F.R. § 248.201 (2013).

<sup>12</sup> *Id.*

63. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

#### **D. Value of Personal Identifiable Information**

64. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>13</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>14</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>15</sup>

65. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

66. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to

---

<sup>13</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Nov. 17, 2023).

<sup>14</sup> *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed June 15, 2023).

<sup>15</sup> *In the Dark*, VPNOOverview, 2019, available at: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Nov. 17, 2023).

change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>16</sup>

67. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

68. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."<sup>17</sup>

69. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information

---

<sup>16</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Nov. 17, 2023).

<sup>17</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Nov. 17, 2023).

compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—one’s Social Security number.

70. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, PII and Social Security numbers are worth more than 10x on the black market.”<sup>18</sup>

71. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

72. The fraudulent activity resulting from the Data Breach may not come to light for years.

73. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>19</sup>

74. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant’s data security

---

<sup>18</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Nov. 17, 2023).

<sup>19</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Nov. 17, 2023).

system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

75. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

76. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's network, amounting to potentially tens of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

77. To date, Defendant has offered Plaintiff and Class Members only twelve months of complimentary identity monitoring services through Experian. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

78. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

79. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

#### **E. Plaintiff Valencia C. Davis' Experience**

80. Plaintiff was Defendant's customer.

81. In order to receive banking services, Defendant was required to provide and did provide her PII to Defendant during the course of his business with Defendant. The PII included her name, Social Security Number, and other financial information.

82. Plaintiff received a Notice of Data Security Incident on or around November 18, 2023. In relevant part, it stated:

**What Happened?** We recently discovered an unauthorized third party gained access to our computer network. Upon identifying the issue, we immediately took steps to contain and remediate the issue, including initiating an internal investigation and notifying law enforcement. We also engaged a forensic security firm to assist with our investigation and confirm the security of our computer systems. The forensic investigation recently concluded and determined that an unknown, unauthorized third party gained access[] to Cinfed's internal corporate network from September 22, 2023 to September 25, 2023 and, during that time, accessed certain documents in our network.

**What Information Was Involved?** We reviewed the contents of the documents and on October 23, 2023, determined that they may have contained your name, Social Security number, and financial account number.

83. To date, Cinfed has done next to nothing to adequately protect Plaintiff Paige and Class Members, or to compensate them for their injuries sustained in this Data Breach.

84. Defendant's Notice of Data Security Incident downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack.

85. Plaintiff and Class Members have been further damaged by the compromise of their PII.

86. Plaintiff's PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed Cinfed's network for the specific purpose of targeting the PII.

87. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

88. Plaintiff stores any documents containing her PII in a safe and secure location, and she diligently chooses unique usernames and passwords for her online accounts.

89. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

90. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining employment from Defendant, which was compromised in and as a result of the Data Breach.

91. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

92. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security Number, being placed in the hands of criminals.

93. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when he began employment with Defendant. Plaintiff, however, would not have entrusted her PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

94. As a result of the Data Breach, Plaintiff Paige anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

### **CLASS ACTION ALLEGATIONS**

95. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated (“the Class” or “Class Members”).

96. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

**All persons Cinfed identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the “Class” or “Class Members”).**

97. Where appropriate, the Class shall be referred to collectively as the “Class” or “Class Members.”

98. Excluded from the Class are Defendant’s officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

99. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

100. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 58,000 individuals.

101. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their PII;
- f. Whether Defendant breached its duty to Class Members to safeguard their PII;
- g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- h. Whether Defendant should have discovered the Data Breach sooner;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant's actions, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- l. Whether Defendant breached a fiduciary duty to Plaintiff and Class Members;
- m. Whether Defendant violated the consumer protection statute invoked below;
- n. Whether Defendant breach implied or express contracts with Plaintiff and Class Members;

- o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;
- p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;
- q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

102. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

103. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions.

104. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

105. **Superiority**. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

106. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

### **CAUSES OF ACTION**

#### **FIRST COUNT**

##### **Negligence**

##### **(On Behalf of Plaintiff and the Class)**

107. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

108. Defendant required customers and employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing services and/or employment.

109. By collecting and storing this data in its computer property, and sharing it and using it for financial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

110. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

111. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to the FTCA, the Ohio Consumer Sales Practices Act ("CSPA"), and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

112. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

113. Similarly, Defendant had a duty to employ reasonable security measures under the CSPA, R.C. 1345.01, *et seq.*, which prohibits "unfair or deceptive acts or practice in connection with a consumer transaction. Such an unfair or deceptive act or practice by a supplier violates this section whether it occurs before, during, or after the transaction." R.C. 1345.02(A). In construing the CSPA, "court[s] shall give due consideration and great weight to federal trade commission orders, trade regulation rules and guides, and the federal courts' interpretations of subsection 45 (a)(1) of the "Federal Trade Commission Act," 38 Stat. 717 (1914), 15 U.S.C.A. 41, as amended." R.C. 1345.02(C).

114. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

115. Furthermore, by requiring customers and employees to provide their PII, Defendant assumed a legal duty to exercise reasonable care in handling and/or storing that PII.

116. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Failing to have in place mitigation policies and procedures;
- e. Allowing unauthorized access to Class Members' PII;
- f. Failing to detect in a timely manner that Class Members' PII had been compromised; and
- g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

117. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security

was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial industry.

118. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

119. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

120. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**SECOND COUNT**  
***Negligence Per Se***  
**(On Behalf of Plaintiff and the Class)**

121. Plaintiff repeats and re-alleges each and every allegation contained the Complaint as if fully set forth herein.

122. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

123. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the PII at issue in this case—including Social Security numbers.

124. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

125. Plaintiff and members of the Class are within the class of persons that the FTC Act was intended to protect.

126. Similarly, Defendant had a duty to employ reasonable security measures under the CSPA, R.C. 1345.01, *et seq.*, which prohibits "unfair or deceptive acts or practice in connection with a consumer transaction. Such an unfair or deceptive act or practice by a supplier violates this section whether it occurs before, during, or after the transaction." R.C. 1345.02(A). In construing the CSPA, "court[s] shall give due consideration and great weight to federal trade commission orders, trade regulation rules and guides, and the federal courts' interpretations of subsection 45 (a)(1) of the "Federal Trade Commission Act," 38 Stat. 717 (1914), 15 U.S.C.A. 41, as amended." R.C. 1345.02(C).

127. Plaintiff and Class Members are within the class of persons the CSPA was intended to protect.

128. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and CSPA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

129. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and members Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity

costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;(vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

130. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession.

**THIRD COUNT**  
**Breach of Fiduciary Duty**  
**(On Behalf of Plaintiff and the Class)**

131. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

132. In light of the special relationship between Defendant and Plaintiff, whereby Defendant became guardians of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its customers, including Plaintiff and Class Members, as follows: (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a data

breach and disclosure; and (3) to maintain complete and accurate records of what customer information Defendant did and does store.

133. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure the PII of its customers and employees.

134. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

135. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

136. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

137. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

138. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

139. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

140. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

141. As a direct and proximate result of Defendant's breaching its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

**FOURTH COUNT**  
**Intrusion Upon Seclusion/Invasion of Privacy**  
**(On Behalf of Plaintiff and the Class)**

142. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

143. Plaintiff and Class Members have a reasonable expectation of privacy in their PII.

144. Defendant's negligent, reckless, and intentional conduct as alleged herein invaded Plaintiff's and the Class Members' privacy.

145. By knowingly failing to keep Plaintiff's and Class Members' PII safe, and by knowingly misusing said information, Defendant negligently, recklessly, and intentionally invaded Plaintiff's and Class Members' privacy by Intruding into Plaintiff's and Class Members' private affairs, without approval, in a manner that would be highly offensive and objectionable to a person of ordinary sensibilities.

146. Defendant knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendant's negligent, reckless, and intentional actions highly offensive and objectionable.

147. Such an intrusion into Plaintiff's and Class Members' private affairs is likely to cause outrage, shame, and mental suffering because the PII disclosed includes financial information, that is only shared with others when an individual is comfortable, as well as sensitive personal information like Social Security Numbers that allow third parties to commit fraud and identity theft.

148. Defendant invaded Plaintiff and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private life by negligently, recklessly, and intentionally misusing their PII without their informed, voluntary, affirmative, and clear consent.

149. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused their PII without their informed, voluntary, affirmative, and clear consent.

150. As a proximate result of such intentional misuse, Plaintiff's and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that a person with ordinary

sensibilities would consider Defendant's intentional actions or inaction highly offensive and objectionable.

151. In failing to protect Plaintiff's and Class Members' PII, and in negligently, recklessly, and intentionally misusing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept secure, confidential, and private. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

**FIFTH COUNT**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiff and the Class)**

152. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

153. When Plaintiff and Class Members provided their PII to Cinfed in exchange for Defendant's services and/or as part of the employment relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information. This duty was separate from that conferred by statute or common law.

154. Defendant solicited and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

155. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

156. Customers who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Similarly, employees

who gave their PII as a condition of the employment relationship, expected Defendant to act reasonably to keep its employees' PII safe. Defendant failed to do so.

157. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

158. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

159. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

160. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

161. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

162. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**SIXTH COUNT**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Class)**

163. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

164. This count is plead in the alternative to Count 6 (breach of implied contract).

165. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant money for banking services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

166. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

167. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

168. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

169. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

170. Plaintiff and Class Members have no adequate remedy at law.

171. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft

of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to effortsspent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continuedrisk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measuresto protect PII in their continued possession; and (vii) future costs in terms of time, effort,and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

172. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

173. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff as ClassRepresentative and her counsel as Class Counsel;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees.

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury on all claims so triable.

Respectfully Submitted,

Dated: November 22, 2023

/s/ Phil Krzeski  
Philip J. Krzeski (0095713)  
**CHESTNUT CAMBRONNE PA**  
100 Washington Avenue, Suite 1700  
Minneapolis, MN 55401-2138  
Telephone: (612) 339-7300  
Facsimile: (612) 336-2940  
*pkrzeski@chestnutcambronne.com*